International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol. 2 Issue 6 May 2016

Enhanced Data Security From Single Clouds To Multiclouds

Sarita Bansod
Department of Computer Science and Engg., University of RGPV, Bhopal, India
sarubansod@gmail.com

ABSTRACT: Cloud is an emerging technology that stores the necessary data and electronic form of data is produced in gigantic quantity. It is vital to maintain the efficacy of this data the need of data recovery services is highly essential.
Cloud computing is anticipated as the vital foundation for the creation of IT enterprise and it is an impeccable solution to move databases and application software to big data centers where managing data and services is not completely reliable.
Our focus will be on the cloud data storage security which is a vital feature when it comes to giving quality service.
It should also be noted that cloud environment comprises of extremely dynamic and heterogeneous environment and because of high scale physical data and resources, the failure of data centre nodes is completely normal.
Therefore, cloud environment needs effective adaptive management of data replication to handle the indispensable characteristic of the cloud environment. Disaster recovery using cloud resources is an attractive approach and in this paper we propose data replication strategy which attentively helps to choose the data files for replication and the strategy proposed tells dynamically about the number of replicas and effective data nodes for replication.
Thus, the purpose of proposed algorithm is useful to help users collect the information from a remote location where network connectivity is absent and secondly to recover files in case it gets deleted or wrecked because of any reason. Even time related problems are also getting resolved so in less time recovery process is executed.

KEYWORDS: cloud computing, disaster recovery, cloud resources, cloud environment, data replication, recovery process

INTRODUCTION:

There are ample of definitions that describe cloud computing and all these definitions agree on how they can offer services to the network users. Cloud computing is storing, accessing and retrieving data or programs over an internet connection using the computer technology. Cloud is delivery of the on demand computing resources. It means using the computing resources like hardware or software that are available on demand as a service over the internet.

It offers end number of services to the users of the network like, storage, operations of different kinds, remote printing and a lot more. Usually it involves the internet supplying vigorously ductile and most of all virtualized resources.

When it comes to business, they run all types of applications on the cloud and cloud computing can be explained as the technology which keeps the data and use in different application and it is controlled remotely without the requirement of downloading some applications on the computers.

A few possible advantages which apply to almost all kinds of cloud computing involves the following:

1. Cost effectiveness: With the use of operational expenses to enhance computing abilities organizations can reduce greatly on the capital expenses.

2. Scalability: Companies can extend from small deployment to large scale deployment and then scale back if required. The scalability of cloud computing help the organizations to make use of extra resources in the peak times so that can help them to meet the diverse consumer needs in the best way.

3. Dependability: Services that make use of several superfluous sites can help in business progression and disaster recovery.

4. Trim down maintenance: The cloud service providers perform system maintenance which doesn't need the installation of application on the computer and the need of maintenance is trimmed down to a great extent.

5. Mobile availability: The moveable workers have elevated productivity because a system can be accessed from anywhere in an infrastructure.

6. Complete clarity or transparency: The extra servers which need to be included to provisioned service with no interruption to the service or need reconfiguration of the application delivery solution. In case the application delivery solution is integrated with the help of management API, then clarity or transparency is reached because of the automated provisioning and de-provisioning of the resources.

Information Security can be seen combining the three objectives that are access control, secured communications, and security of private data. Information security is also described as the protection of private data and processing from unauthorized observation, modification, or interference.

The main aim is to offer more scalable services to the users in a transparent way that comes at a cheap price, is extremely flexible and properly available as a robust computing resource. The Software as a Service (SaaS) architecture offers the software applications hosted and managed by a service provider to the end-user and this is useful to replace the applications run locally with the use of web services applications.

In the Infrastructure as a Service (IaaS), service includes managing the hardware and software for processing, data storage, networks and any required infrastructure for deployment of operating systems and applications that is required normally in a data center which is managed by the user. In the Platform as a Service (PaaS), service includes programming languages and tools and an application delivery platform that is hosted by the service provider which is useful for support development and delivery of the end-user applications.

Related Work (Litrature Survey):

We propose an adaptive flexible replication strategy in a cloud environment that is highly scalable and has the potential to manage the problems listed below effectively:

 What needs to be replicated that can help the non-functional QoS to improve? The chosen procedure mainly depends on scrutinizing the data requests history with the help of lightweight time-series prediction algorithm. On using this predicted data request, we can understand which of the data files require replication that can help to enhance the system dependability.

 The amount of replicas of every data that is chosen

 The position of the new replicas that are on the available data centers.

 The overhead of replication strategy on the Cloud infrastructure. It is a very crucial factor of the proposed adaptive replication strategy where the Cloud has a big amount of data centers as well as a big scale data.

Thus, the adaptive replication strategy should be a lightweight strategy. The offered adaptive replication strategy is made on the fact that the lately most accessed data files will be accessed again in the near future as per the collected prediction statistics of the files access pattern. A replication factor is then determined depending on a data block and the availability of each replica that is present need to pass a predetermined threshold, so the replication operation will be triggered. A new replica is then established on a new node which helps to get a better replication factor. The amount of new replicas will be then calculated adaptively depending on improving the availability of every file analytically. Though, the lightweight time-series algorithm will be executed for predicting the future requests of the data files. The decision about replication basically depends on the offered predictions. The heuristic proposed for the dynamic replication strategy is analytically cheap, and it has the ability to handle large scale resources and data in the moderate time frame.

FUTURE WORK

Modules Description

The figure 1 shows the data recovery model where the Remote Data Backup server is a type of server that helps to store the complete data of the main cloud as a whole and it is positioned at a remote place that is far away from cloud. And in case the data is lost because of central repository then its remote repository uses the information. The objective is to assist clients to collect the information from remote repository if by chance the network connectivity is not there or the main cloud is not able to give the data to the clients. As shown in the Fig 1, if clients find that data is not there on the central repository, then clients are free to access the files from a remote repository (i.e. indirectly).

The Remote backup services will handle the following problems effectively:

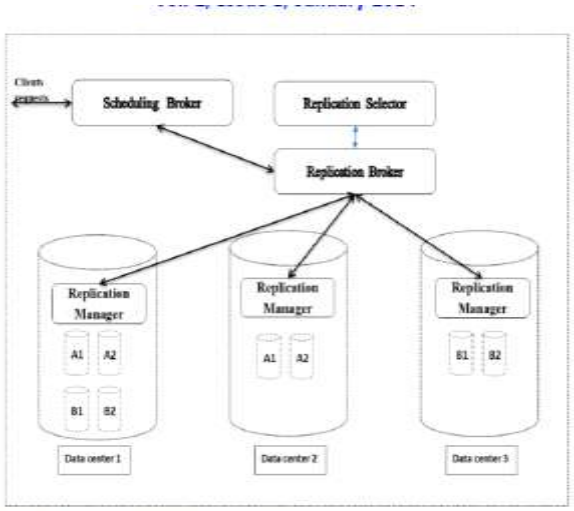
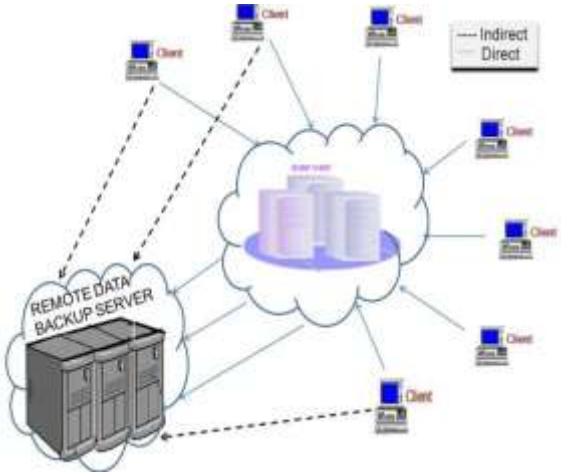


Fig.1. The Cloud data server architecture.

1) Security concerns or privacy and ownership.

2) Server relocation to the cloud.



3) Security of data

4) Dependability.

5) Cost efficacy.

6) Correct or proper timing.

1) Security concerns or privacy and ownership.

There are many different clients who access the cloud using their login details which are different for every client and the authentication process also varies here. The clients are free to upload their private as well as important data on the cloud. Thus, the privacy and ownership of the data needs to be maintained. The data owner should be able to access their private data and must be able to read, write or perform any other operation. The remote server should be able to offer this privacy and ownership.

2) Server Relocation

For the recovery of data the need of relocation of server to the cloud is highly important. The server relocation means transferring the data of the main server to another server, but the new location is not known to the client. The clients get the data in a similar manner where there is no intimation of relocation of the main server so the location clarity or transparency is offered to the clients and to the third party by the time the data is being shifted to the remote server.

3) Security of data

The data of the client is stored safely at the central repository. Such type of security needs to be followed in its remote repository also. In remote repository, the data needs to be protected completely so that there is no access or destruction caused to the remote cloud's data either intentionally or unintentionally either by third party or by any other client.

4) Dependability

The remote cloud should retain all the dependability characteristics. It is because in cloud computing the main cloud keeps the complete data and every client depends on the main cloud for each and every small amount of data. Thus, it is vital that the cloud and remote backup cloud should perform a trustworthy role. This means that both the servers should be able to offer data to the client as soon as possible when they need it from the main cloud or a remote server.

5) Cost Efficacy

The price for the execution of the remote server and its recovery as well as back-up technique also play an important role when the main cloud and its correspondent remote cloud structure is being created. The price for constituting the remote setup and implementing the technique should be minimal so the small business is able to pay for such system and large business can spend minimum cost as possible.

6) Correct or proper timing

The data recovery procedure consumes some time for retrieving the data from remote repository as this remote repository is quite far from the main cloud and its clients. Therefore, the time taken for such retrieval should be as short as it can be so the client can get the data as early as possible without keeping in consideration how far the remote repository is from the client.

CONCLUSION:

The use of cloud computing in enhancing rapidly and users do not want to lose on their private information and cloud computing security is considered to be a major concern. To offer a protected environment and secure the sensitive dynamic or static data on cloud computing, first of all various types of threats are highlighted and then the proposed cloud computing security solution is offered and explained so the safety of the user and clients can be enhanced. The proposed model advantages are also explained in detail and how it can achieve high safety. The solution offered with the cloud computing proposed approach there is better security and risk management along with deploying standard information security policies can b executed smoothly.

REFERENCES:

[1] Radha1 , Dr. Rekha Patil, Load Balancing with Disaster Recovery using Multi Cloud, Department of Computer Science and Engineering M.Tech (CSE), Poojya Doddappa Appa College of Engineering, Gulbarga, Karnataka, India

[2] Sayali S. Satav, Ganesh Prajapati, Sonali Dahiphale, Sadhana More, Prof.N Bogiri, Cloud Computing Security: From Single Cloud to Multi-Clouds using Digital Signature International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Pune Volume 4 Issue 4, April 2015

[3] Sangeeta N Dhamdhare, Cloud computing and virtualization technologies in libraries, Modern technologies of Arts, science and commerce, India

[4] Assoc. Prof., Data Integrity in cloud computing security Faculty of Information Technology, Computer Science Dept., Applied Science University, Amman-Jordan, vol 58, No 3, 31st December, 2013.

[5] Rajiv R.Bhandari, Mishra N., Encrypted IT Auditing and Log Management on Cloud Computing, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, pp. (302), September 2011.